HOW TO PREVENT RANSOMWARE AND PROTECT YOUR BUSINESS

Table Of Contents

How to Prevent Ransomware and Protect Your Business

Business owners and managers have to focus on a variety of elements to ensure the success of their organization, including cybersecurity. Each year, there are **more than 188 million** ransomware attacks, and a large percentage target small and medium-sized businesses (SMBs). Research suggests that the average cost of a ransomware attack can **exceed $10,000,** but this number doesn't include the loss due to production delays or customer churn, which means that this value is often much higher.

Creating a safe environment for clients and employees should be a priority for all companies, regardless of the industry. More than 70% of ransomware attacks **target small and medium-sized organizations** because these companies are more vulnerable -- and these threats are growing every year.

From creating a culture that centers around security to implementing tools that help prevent ransomware attacks, companies need to take a variety of steps to ensure all areas are protected against cybercriminals.

What is Ransomware?

Business owners and managers have to focus on a variety of elements to ensure the success of their organization, including cybersecurity. Each year, there are more than 188 million ransomware attacks, and a large percentage target small and medium-sized businesses (SMBs).

Research suggests that the average cost of a ransomware attack can exceed $10,000, but this number doesn't include the loss due to production delays or customer churn, which means that this value is often much higher.

Creating a safe environment for clients and employees should be a priority for all companies, regardless of the industry. More than 70% of ransomware attacks target small and medium-sized organizations because these companies are more vulnerable -- and these threats are growing every year.

From creating a culture that centers around security to implementing tools that help prevent ransomware attacks, companies need to take a variety of steps to ensure all areas are protected against cybercriminals.

How Does Ransomware Affect Your Business?

Despite the fact that some forms of cybercrime are as old as the internet itself, the first cases of ransomware were first reported in 2005. Since then, cybercriminals have developed more sophisticated forms of ransomware, which has resulted in an increase in attack frequency and severity.

To successfully fight ransomware, businesses must implement comprehensive security practices that protect them against conventional and new types of attacks. Companies also need to develop internal resources and take the time to train team members about the most common ways these attacks are carried out. This can help raise awareness and reduce the chances of falling victim to this type of cyberattack.

The type of code and exact method can vary from one case to another, but most ransomware attacks follow similar stages. These are:

First Contact

The first contact is the original message or email that contained the ransomware code. In most cases, these malicious parties use social engineering to create messages that look legitimate, which entices the user to open the link or download the attached file. The file or link contains the malicious code, which infects the device and, potentially, other machines in the network.

According to some estimates, 94% of cyber attacks, in general, occur via email. However, more companies are adopting alternative methods like social media and instant messages, so it's important to monitor and safeguard all communication channels in place.

Beginning of the Attack

The attack begins a few seconds after the user clicks on the link or downloads the attachment in the malicious message. At this point, the virus will start infecting different files in the same device and will go undetected if there isn't a robust security system in place.

If the right system is in place, organizations can limit the movement of the virus, detect any suspicious activity, and take action before the virus has time to move on to the following stages.

Infection

Depending on the type of virus and what it was designed to do, it may start tracking down essential files, disabling recovery mechanisms, and rendering backups useless. The time it takes to complete this stage will vary depending on how many files are stored in the device, so having a robust security system in place can slow the infection and broaden the reaction window.

Encryption

Once it's infected the device, the malicious code will take control and begin the file encryption process. Additionally, this is the stage where the piece of ransomware established contact with the perpetrator, which allows the deceitful party to control the virus remotely. This is the same connection that the perpetrators use to provide access once the ransom has been paid

Spreading

Ransomware attacks are designed to exploit additional weaknesses and infect other machines in different forms. If the network is not protected or segmented into different parts, the malicious code will begin to spread to other devices using the same connection. In SMBs, this can affect the entire team and completely halt operations until the matter is solved.

Can Small and Medium-Sized Businesses Fight Ransomware?

For SMBs, the best way to protect their clients and employees from ransomware and other forms of cyberattack is to take preventative measures. Business owners and IT managers need to identify the best ways to create a safe internal ecosystem and stay ahead of the new approaches being developed by malicious entities.

All businesses are unique, so each cyberattack occurs under different circumstances. Each organization needs to design a tailored plan that allows it to protect every device on its network. With this in mind, quality ransomware prevention strategies for SMBs do share some general similarities because they all tend to be:

Effective

While this may seem obvious, companies have to go the extra mile to ensure that the solutions put in place are effective. In other words, businesses should ensure that the different steps they take will actually help prevent ransomware. This applies to the entire strategy put in place, so managers need to create and evaluate security training materials to ensure the delivery of accurate content that's functional and easy to understand.

In addition to the above, managers also assess the security tools they choose and ensure they actually work. All security software providers will ensure that their platform is the best, but decision-makers need to check the different features available, speak to the support team, and find other ways to identify the best solutions.

Comprehensive

Ransomware attacks are designed to be effective even if team members commit a relatively small mistake like clicking on the wrong link. The best prevention mechanisms provide comprehensive protection for all potential attack points in order to stop malicious code from exploiting any weaknesses in the network.

In addition to protecting from sophisticated attacks, comprehensive security systems also simplify management and maintenance. Companies that opt for low-tier solutions that don't provide comprehensive coverage often need to leverage multiple platforms. This can exponentially increase the amount of time needed to monitor and manage these solutions, affecting the overall efficiency of your company.

Easy to Implement

It's common for SMBs to have IT limitations in terms of team size and capacity. IT team members have to focus on a variety of essential tasks that often take up most of their time. Furthermore, these team members may not have the tools, resources, or knowledge to properly set up a robust ransomware protection system.

For these reasons, a quality security solution for small and medium-sized companies should be easy to implement. In addition to being simple, the setup should not be time-consuming or difficult to ensure it's accessible to companies of all sizes.

Affordable

Tight budgets and limited resources are two challenges faced by businesses in all industries. Expensive security solutions can put a lot of financial pressure on an organization and force it to overstretch its budget, which ultimately affects other areas including overall performance and profitability.

Robust security solutions for SMBs offer a high level of protection at an affordable price, which allows companies to protect their data and remain competitive at the same time.

Long-Term

Small and medium-sized companies are on a constant quest to grow, so it's important to find a security system that is scalable. If a security platform is only designed for a limited number of team members or devices, companies that achieve their business goals will have to discard these solutions and find new providers down the line, which can ramp up security expenses.

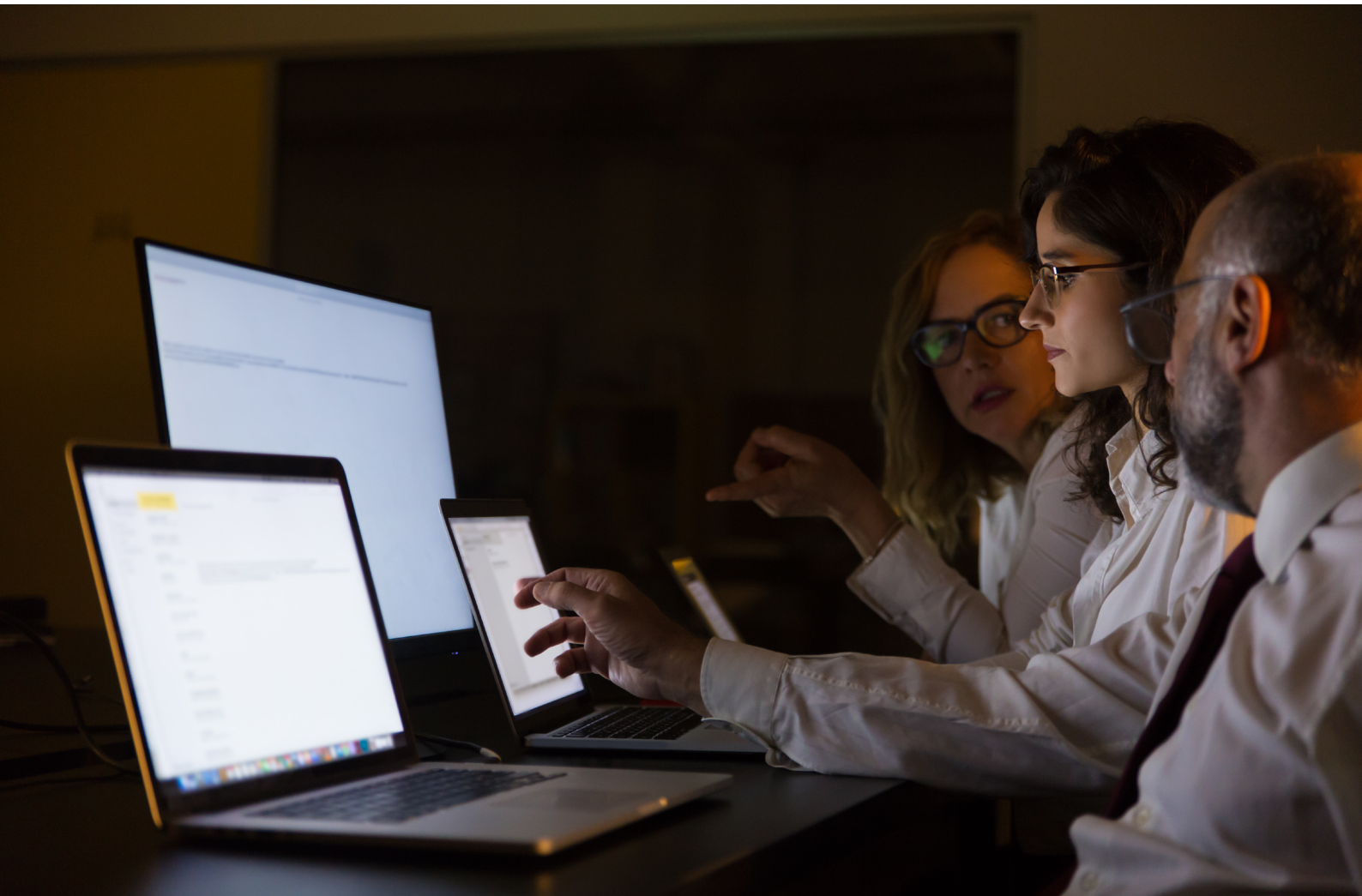
Instead, business owners and managers need to find a security platform that has the ability to grow with their companies. In addition to scalability, it's also important to ensure that the providers are constantly making security improvements to the platforms you choose to stay protected against new types of ransomware attacks.

From a Reputable Security Solutions Provider

There are hundreds of security platforms to choose from, but not all of these provide the same level of protection. In many cases, security platform providers develop solutions that only address one potential threat area. So, companies need to find a wholesome alternative developed by a reputable company that has a proven track record in the cybersecurity industry.

WatchGuard is one of the leading security solution providers that develop powerful tools for companies of all sizes. Through its different products, WatchGuard provides comprehensive security features that help protect SMBs from ransomware and other cyberattacks.

Businesses that leverage these solutions can create a safe ecosystem that allows employees, clients, and partners to employ digital resources with the peace of mind they deserve.



Tips to Prevent Ransomware and Protect Your Business

Implementing a security system that protects against every possible form of malware is impossible because there is always a chance for human error. For this reason, the best approach is to create a multi-layered mechanism where each level works as a security buffer for the next. This will result in higher chances of identifying ransomware before it causes damage, which can save companies a significant amount of time and resources.

Additionally, companies should also create a worst-case scenario plan which will help guide them if they fall victim to ransomware. Paying the ransom is not advisable because it's usually costly and it leaves the door open for additional attacks, so the best approach is to develop a solid security strategy and implement the right tools early on.

Below, we've put together a few tips to help you develop a robust security system for your SMB.

Establish a Security-Focused Mindset

Society as a whole is starting to focus on privacy and cybersecurity more than in previous years, but this doesn't mean that your team members are always thinking about preventing breaches. To ensure that your team is knowledgeable enough to identify potential ransomware attacks, you should provide basic and advanced security training.

Your training materials should include all relevant definitions as well as an explanation about ransomware and how it works. Make sure to include examples of known attacks and what to do in case a team member receives a suspicious message. You should also set aside time

Create Backups on a Frequent Basis

As mentioned previously, ransomware doesn't destroy files but it limits access to these instead, which essentially produces the best results. To recover data quickly, you should frequently create backups of your most essential files and store these in multiple locations.

Remember, sophisticated ransomware attacks can also disable backups, so you should get creative and use a combination of physical on-site devices as well as cloud solutions. And, you should also ensure that these are not on the same network or that the network is segmented to avoid infection.

Keep in mind that the essential files will vary from one company to another, so you should take the time to identify the most valuable documents for your organization. Also, avoid using conventional cloud syncing services like Google Drive as your backup because these may spread the infection even more.

Stop Ransomware from Being Delivered to Team Members

Like all other types of malware, ransomware attacks have a point of origin. This means that companies can reduce the likelihood of being infected by preventing malicious messages from being delivered to their team members. Some of the steps you can take include:

- Setting up an email filtering system that blocks suspicious activity
- Blocking sites that are known for containing malicious code
- Inspecting file and blocking unexpected or suspicious types
- Create triggers that block malware

It's important to note that these steps are often taken at a network level rather than in each individual device, so your IT team needs to know how to implement the security improvements listed above.

Block Deceitful Code from Running on Your Networks and Devices

Even if creating a multi-layered approach, you should assume that you will get infected by malicious code at one point or another. Therefore, you should take precautions to ensure that once the malicious code enters a device it can't infect the host or the rest of the network.

The specific steps needed to block deceitful code vary depending on the software you're running, number of devices, security system in place, and other variants. With this in mind, you should leverage both network and device-level security features that help:

- Limit the applications that run on specific devices
- Detect suspicious activity in real-time
- Implementing a consistent scripting environment

Organizations should also consider installing security updates as soon as they're available to reduce known vulnerabilities. This includes installing the latest versions of operating systems as well as firmware and other applications.

Develop a Plan that Limits the Negative Impact and Allows Fast Response

Sophisticated ransomware can exploit any weaknesses in the security system, even if it's not allowed to run on a specific device. Companies should take additional steps to prevent this malware from spreading to other devices within the network or stealing authentication credentials.

You should also ensure that outdated devices that pose a risk to the rest of the network are not online anymore and maintain an organized log of the different operating systems you're currently working with.

Deploy WatchGuard and Adjust the Settings Properly

WatchGuard is a superb cybersecurity solution that can minimize the chances of experiencing a ransomware attack. That said, if the system isn't set up properly, malicious entities can exploit different vulnerabilities and compromise your data.

If you've implemented WatchGuard to help protect your employee and client information, make sure that all settings are adjusted properly. In addition to increased risk, a poor WatchGuard setup can also slow down your network and affect other parts of its performance. The best way to avoid this issue is to work with a WatchGuard gold partner that can assess the performance of your security system and ensure it's working at full capacity

Fighting On-Going Ransomware Attacks

Ransomware can have a devastating effect on any business, especially small to medium-size companies. If one or more of your devices have been infected with ransomware, you should:

- Disconnect infected devices from the network right away
- Disable core network connections that can reduce the extent
- Reset network credentials, especially those of administrators
- Attempt to restore any available backups, but keep them off your main network
- Contact a cybersecurity specialist to assess whether the ransomware as any exploitable weaknesses and to potentially